





Procesos administrativo



INTRODUCCIÓN

La administración de procesos en Linux es una parte crítica de la gestión del sistema operativo. Un proceso es cualquier programa en ejecución, y la capacidad de gestionar estos procesos de manera eficiente es esencial para mantener un sistema saludable y optimizado. Desde monitorear el rendimiento hasta controlar el uso de recursos, la administración de procesos permite a los administradores de sistemas garantizar que las aplicaciones se ejecuten sin problemas y que el sistema responda adecuadamente a las demandas.

OBJETIVOS

- o Crear un archivo de registro nuevo para las listas de procesos.
- o Utilizar el comando top.
- o Establecer una tarea repetitiva que ejecute los comandos de auditoría anteriores una vez al día.





En esta tarea, se conectará a una instancia EC2 de Amazon Linux.

Utilizará una utilidad SSH para realizar todas estas operaciones.

Las siguientes instrucciones varían ligeramente según si utiliza

Windows o Mac/Linux.

En Linux

o Usando distribución Ubuntu con Subsistema de Windows para Linux (WSL).

```
ec2-user@ip-10-0-10-43:~
leps2408@LAPTOP-1I89QL1A:~$ neofetch
                   .-/+oossssoo+/-
                                                                  leps2408@LAPTOP-1I89QL1A
           +ssssssssssssssss
                                                                  OS: Ubuntu 20.04.6 LTS on Windows 10 x86_64
    .ossssssssssssssssdMMMNysssso.
/ssssssssssshdmmNNmmyNMMMMhssssss/
                                                                  Kernel: 5.15.153.1-microsoft-standard-WSL2
                                                                  Uptime: secs
 +sssssssshmydMMMMMMMddddysssssss+
/sssssssshNMMMyhhyyyyhmNMMMNhssssssss/
                                                                  Packages: 673 (dpkg), 4 (snap)
Shell: bash 5.0.17
.sssssssdMMMNhssssssssshNMMMdsssssss.
+sssshhhyNMMNysssssssssssyNMMMyssssss+
ossyNMMMNyMMhsssssssssssshmmmhssssssso
ossyNMMMNyMMhssssssssssssshmmmhssssssso
                                                                   Theme: Adwaita [GTK3]
                                                                   Icons: Adwaita [GTK3]
                                                                   Terminal: Relay(482)
                                                                   CPU: Intel i5-10300H (8) @ 2.496GHz
sssynningriffissssssssssssnimminsssssso
ssssshhhyNMMNyssssssssssssshNMMMdssssssss.
sssssssshNMMMyhhyyyyhdNMMMNhsssssss/
+ssssssssdmydMMMMMMddddyssssssss+
/ssssssssssshdmNNNNmyNMMMHssssss/
                                                                   GPU: 0929:00:00.0 Microsoft Corporation Device 008e
                                                                   Memory: 421MiB / 3838MiB
      .osssssssssssssssdMMMNysssso
          .+ssssssssssssssssss+:,
                  .-/+oossssoo+/-.
```





o Ubicarse en la carpeta del archivo labuser.pem descargado.

```
leps2408@LAPTOP-1I89QL1A:~$ ls
labsuser.pem labsuser.pem:Zone.Identifier
```

o Cambiar permisos a *labuser.pem* descargado, según el comando.

```
leps2408@LAPTOP-1I89QL1A:~$ chmod 400 labsuser.pem
```

o Conectar con la instancia EC2 de AWS utilizando el IP público IPv4, según el comando.

```
leps2408@LAPTOP-1189QL1A:~$ ssh -i labsuser.pem ec2-user@35.94.49.146
The authenticity of host '35.94.49.146 (35.94.49.146)' can't be established.
ECDSA key fingerprint is SHA256:ropSTchpGPT/u0xCZgDNMY4VOD2vvauVnHu+KovTfGI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.94.49.146' (ECDSA) to the list of known hosts.
```

o Finalmente, se muestra la imagen de la distribución de Amazon Linux 2.

```
/ #_
~\_ ####_ Amazon Linux 2

~~ \#####\
~~ \####| AL2 End of Life is 2025-06-30.

~~ \#/___
~~ \/ ###|

~~ \/ \/ A newer version of Amazon Linux is available!

~~ __/
_/ _/ Amazon Linux 2023, GA and supported until 2028-03-15.
_/m/' https://aws.amazon.com/linux/amazon-linux-2023/
```





En este ejercicio, se crea un archivo de registro a partir del comando ps. Ese archivo de registro debe agregarse a la sección SharedFolders. Cree un archivo de registro denominado processes.csv con ps -aux y omita cualquier proceso que contenga un usuario raíz "[" o "]" en la sección COMMAND.

o Asegurarse de estar en la carpeta CompanyA.

o Mirar los procesos que se encuentran corriendo y filtrar la palabra raíz escribiendo sudo ps -aux | grep -v root | sudo tee SharedFolders/processes.csv.

```
ec2-user@ip-10-0-10-98:~/coi ×
[ec2-user@ip-10-0-10-98 companyA]$ sudo ps -aux | grep -v root | sudo tee SharedFolders/proc
esses.csv
             PID %CPU %MEM
USER
                                          RSS TTY
                                                           STAT START
                                                                           TIME COMMAND
rpc 1712 0.0 0.3 67256
libstor+ 1717 0.0 0.1 12628
dbus 1720 0.0 0.4 58248
                                                                           0:00 /sbin/rpcbind -w
0:00 /usr/bin/lsmd -d
                                         3264 ?
                                                           Ss
                                                                 16:13
                                         1804
                                                           Ss
                                                                 16:13
                                        4068 ?
                                                          Ss
                                                                 16:13
                                                                           0:00 /usr/bin/dbus-daemon --syst
em --address=systemd: --nofork --nopidfile -
                                                        -systemd-activation
          1726 0.0 0.4 96344 4736 ?
                                                                16:13
                                                                           0:00 /sbin/rngd -f --fill-waterm
ark=0 --exclude=jitter
chrony 1732 0.0 0.3 120184
chrony
postfix
                                                                 16:13
                                                                           0:00 /usr/sbin/chronyd -F 2
                   0.0 0.7 90396
0.0 0.7 90468
                                                                           0:00 pickup -l -t unix -u
0:00 qmgr -l -t unix -u
            2161
                                         6824 ?
                                                                 16:13
.
postfix
            2162
                                         6780 ?
                                                                 16:13
ec2-user 2893 0.0 0.4 150624 44460 ?
ec2-user 2894 0.0 0.4 126716 4048 pts/0
                                                                           0:00 sshd: ec2-user@pts/0
0:00 -bash
                                                                 16:17
                                                               16:17
[ec2-user@ip-10-0-10-98 companyA]$ |
```





o Confirmar con cat SharedFolders/processes.csv.

```
ec2-user@ip-10-0-10-98:~/coi ×
[ec2-user@ip-10-0-10-98 companyA]$ cat SharedFolders/processes.csv
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
USER
rpc 1712 0.0 0.3 67256 3264 ?
libstor+ 1717 0.0 0.1 12628 1804 ?
dbus 1720 0.0 0.4 58248 4068 ?
                                                                                                        Ss 16:13
Ss 16:13
                                                                                                                                     0:00 /sbin/rpcbind -w
0:00 /usr/bin/lsmd -d
                                                                                                        Ss
                                                                                                                   16:13
                                                                                                                   16:13
                                                                                                                                     0:00 /usr/bin/dbus-daemon --syst
                                                                                                        Ss
dbus 1720 0.0 0.4 58248 4068 ? Ss 16:13 0:00 em --address=systemd: --nofork --nopfile --systemd-activation rngd 1726 0.0 0.4 96344 4736 ? Ss 16:13 0:00 ark=0 --exclude=jitter chrony 1732 0.0 0.3 120184 3088 ? S 16:13 0:00 postfix 2161 0.0 0.7 90396 6824 ? S 16:13 0:00 postfix 2162 0.0 0.7 90468 6780 ? S 16:13 0:00 ec2-user 2893 0.0 0.4 150624 4460 ? S 16:17 0:00 ec2-user 2894 0.0 0.4 126716 4048 pts/0 Ss 16:17 0:00
                                                                                                     Ss 16:13 0:00 /sbin/rngd -f --fill-waterm
                                                                                                                                      0:00 /usr/sbin/chronyd -F 2
                                                                                                                                     0:00 pickup -l -t unix -u
0:00 qmgr -l -t unix -u
0:00 sshd: ec2-user@pts/0
                                                                                                                                      0:00 -bash
 [ec2-user@ip-10-0-10-98 companyA]$ |
```





En este ejercicio, se utilizará el comando *top*. Ejecutar el comando *top* para mostrar los procesos e hilos que están activos en el sistema y observar las salidas con el comando *top*.

o Ingresar el comando *top*. Nota: 87 tareas se encuentran en total, 1 (running), 47 (sleeping)

© ec2	-user@ip-	-10-0-10-98:~	/coi >	< + ~								X
top - 16:31:18 up 18 min, 1 user, load average: 0.00, 0.00, 0.00 Tasks: 87 total, 1 running, 47 sleeping, 0 stopped, 0 zombie %Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 99.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.2 s KiB Mem : 966808 total, 361264 free, 72888 used, 532656 buff/cache KiB Swap: 0 total, 0 free, 0 used. 751584 avail Mem											ř	
PID	USER	PR	NI	VIRT	RES	SHR S	%CPU		TIME+ COMMAN			
1	root	20	0	123504	5432	3920 S	0.0	0.6	0:01.31 system	d		
2	root	20	0	Θ	0	0 S	0.0	0.0	0:00.00 kthrea			
4	root		-20	0	0	0 I	0.0	0.0	0:00.00 kworke			
	root		-20	0	0	0 I	0.0	0.0	0:00.00 mm_per			
7	root	20	0	0	0	0 S	0.0	0.0	0:00.04 ksofti			
	root	20	0	0	0	0 I	0.0	0.0	0:00.04 rcu_sc			
	root	20	0	0	0	0 I	0.0	0.0	0:00.00 rcu_bh			
	root	rt	0	0	0	0 S	0.0	0.0	0:00.00 migrat			
	root	rt	0	0	0	0 S	0.0	0.0	0:00.00 watchd			
	root	20	0	0	0	0 S	0.0	0.0	0:00.00 cpuhp/			
	root	20	0	0	0	0 S	0.0	0.0	0:00.01 cpuhp/			
	root	rt	0	0	0	0 S	0.0	0.0	0:00.00 watchd			
	root	rt	0	0	0	0 S	0.0	0.0	0:00.19 migrat			
	root	20	0	0	0	0 S	0.0	0.0	0:00.02 ksofti			
	root	20	0	0	0	0 I	0.0	0.0	0:00.03 kworke			
	root		-20	0	0	0 I	0.0	0.0	0:00.00 kworke			
	root	20	0	0	0	0 S	0.0	0.0	0:00.00 kdevtm	pfs		
	root		-20	0	0	0 I	0.0	0.0	0:00.00 netns			
22	root	20	0	0	0	0 I	0.0	0.0	0:00.01 kworke	r/u4:1		
	root	20	0	0	0	0 S	0.0	0.0	0:00.00 khungt			
202	root	20	0	Θ	0	0 S	0.0	0.0	0:00.00 oom_re			
203	root	0	-20	0	0	0 I	0.0	0.0	0:00.00 writeb	ack		
204	root	20	0	0	0	0 S	0.0	0.0	0:00.00 kcompa	ctd0		

o Para salir, presionar *q*. Probar el comando *top -hv* para encontrar información de uso y versión.









En este ejercicio, creará un trabajo cron que generará un archivo de auditoría con ##### para cubrir todos los archivos .csv. Recuerde que cron es un comando que ejecuta una tarea de forma regular a una hora determinada

• Validar que se encuentra en la carpeta CompanyA, ingresar pwd.

o Ingresar sudo crontab —e para crear un espacio de trabajo. Ingresar al modo de inserción. Ingresar SHELL=/bin/bash, luego PATH=/usr/bin:/bin:/usr/local/bin, en la siguiente línea MAILTO=root, y finalmente en la última línea se ingresa 0 * * * * ls -la \$(find .) | sed -e 's/..csv/#####.csv/g' > /home/ec2-user/companyA/SharedFolders/filteredAudit.csv





o Guardar el archivo y confirmar con sudo crontab -l.

